Poster: Privacy in Distributed Economic Dispatch in Smart Grid

Avikarsha Mandal
Offenburg University of Applied Sciences
Offenburg, Germany
avikarsha.mandal@hs-offenburg.de

Erik Zenner
Offenburg University of Applied Sciences
Offenburg, Germany
erik.zenner@hs-offenburg.de

***Abstract*—The aim of the smart grid is to achieve more efficient, distributed and secure supply of energy over the traditional power grid by using a bidirectional information flow between the grid agents (e.g. generator node, customer). One of the key optimization problems in smart grid is to produce power among generator nodes with a minimum cost while meeting the customer demand, known as Economic Dispatch Problem (EDP). In recent years, many distributed approaches to solve EDP have been proposed. However, protecting the privacy-sensitive data of individual generator nodes has been largely overlooked in the existing solutions. In this work, we show an attack against an existing auction-based EDP protocol considering a non-colluding semi-honest adversary. We briefly introduce our approach to a practical privacy-preserving EDP solution as our work in progress.**

1. Introduction

The traditional power grid is going through some major infrastructural changes to become *smarter* since the last decade [4]. The smart grid proposes a bidirectional communication network on top of the existing energy network to make the grid more efficient and reliable. However, it is important that while building new protocols for smart grid, the privacy risks involved must be addressed and mitigated. The Economic Dispatch Problem (EDP) is one of the fundamental optimization problems in the power grid community [2] [6]. The EDP solution gives a power output combination of all generator nodes which achieves minimum operating cost while supplying the demand to the customers. The total cost of operation can be formulated as:

$$C_{total} = \sum_{i=1}^{n} C_i(x_i) \tag{1}$$

The notation used in our work is given in TABLE 1. The objective of the EDP is to find optimal values for all x_i's such that C_{total} is minimum. Furthermore, an EDP solution should maintain the demand (2) and generator (3) constraints as follows:

$$D - \sum_{i=1}^{n} x_i = 0 \tag{2}$$

$$\underline{x_i} \leq x_i \leq \overline{x_i} \tag{3}$$

Notation	Description
n	Total number of generator nodes
$i, j, \bar{i}, \bar{j}$	Different generator nodes
$\mathcal{A}$	Non-colluding semi-honest attacker
t	Discrete time step index
x_i	Output power of node i
$x_i(t)$	Output power of node i at round t
C_i	Cost function of node i
a_i, b_i, c_i	Cost function parameters for quadratic convex part
e_i, d_i	Cost function parameters for non-convex part
D	Total power demand for customers (public)
$\underline{x_i}$, $\overline{x_i}$	Minimum and maximum output power limit of i
s	Scalar parameter (public)
π_i, μ_i	Auction bids from node i

TABLE 1. NOMENCLATURE

The demand and generator constraints are straightforward as total power generation should be equal to the demand and a generator node can not produce beyond its generation limits. In recent years, instead of central EDP calculation, many distributed EDP algorithms have been proposed in context of the smart grid [2] [6]. However, the privacy risks associated while sharing information with other nodes is a major concern [5]. For example, revealing one generator node's cost function parameters, output power and generator constraints to an another node can give the competitor node a crucial advantage in the energy market. In a competitive energy market, a competitor can outplay its victim (knowing the auction bids from the victim's cost function). The distributed EDP solution techniques can vary with the type of the cost function used. Conventionally, the cost function used in EDP is modelled as a quadratic convex function as follows [6]:

$$C_i(x_i) = a_i x_i^2 + b_i x_i + c_i \tag{4}$$

As mentioned in [5], the privacy-sensitive data for quadratic convex EDP are a_i, b_i, c_i, $x_i(t)$, $\underline{x_i}$ and $\overline{x_i}$. Realistically, a sinusoidal term $|d_i \sin(e_i(\underline{x_i} - x_i))|$ is often added to the cost function with some non-differentiable points making the function non-convex [2]. In our previous work [5], a private protocol for EDP calculation has been proposed for a quadratic convex cost function.

2. Analysis of Binetti et al. [2]

Binetti et al. proposed an auction-based distributed consensus protocol to solve EDP in [2]. Whereas another existing consensus approach based on a lamda-iteration method [6] requires a smooth quadratic convex cost function, the auction-based protocol from Binetti et al. is also applicable to non-convex cost functions.

2.1. Original Protocol from Binetti et al.

For simplicity, we consider a fully connected network of generator nodes. The core idea of the Binetti et al. protocol is based on *double auction*, where each node can act as both buyer and seller. The power output of each node is changed by negotiating with other nodes. Initially, every node knows a public scalar parameter $s \in \mathbb{R}$ for searching optimal values. At every time instance t, each node i generates two output bids as follows:

$$\pi_i(t) = C_i(x_i(t) + s) - C_i(x_i(t))$$

$$\mu_i(t) = C_i(x_i(t)) - C_i(x_i(t) - s)$$

The $\pi_i(t) \in \mathbb{R}$ value denotes the estimated increase in cost for the increase of power output $x_i(t)$ to $x_i(t) + s$. The $\mu_i(t) \in \mathbb{R}$ is the amount of save in cost for the reduction of current power $x_i(t)$ to $x_i(t) - s$. Zero bids are placed if increase or reduction of power violates the generator constraint equation (3). Then, each node i sends its own bid $\pi_i(t)$ (bid π) and $\mu_i(t)$ (bid μ) to its neighbours. The node who has the lowest value for $\pi_i(t)$ ($\pi_i(t) > 0$) wins the bid π and the node who has the highest value for $\mu_i(t)$ ($\mu_i(t) > 0$) wins the bid μ. Hence, the winner bidder $\bar{i}$ is the node who can generate extra s amount of power with the lowest cost. On the contrary, the winner bidder $\bar{j}$ is the node who can save maximum amount cost with producing less s amount of power. Finally, the winner bidders $\bar{i}$ and $\bar{j}$ calculate $\delta = \mu_{\bar{j}}(t) - \pi_{\bar{i}}(t)$. If $\delta > 0$, the exchange of s amount of power will lead to a save of amount δ. Therefore, if $\delta > 0$, the update rule for $\bar{i}$ and $\bar{j}$:

$$x_{\bar{i}}(t+1) = x_{\bar{i}}(t) + s$$

$$x_{\bar{j}}(t+1) = x_{\bar{j}}(t) - s$$

The algorithm iterates until no exchange of s amount of power between two nodes will lead us to a low-cost solution. Furthermore, the demand constraint (Eq (2)) is maintained as $D = \sum_{i=1}^{n} x_i(t)$ at any time t instance.

2.2. Attack Sketch: Privacy-sensitive Data Leakage

In our attacker model, we consider a non-colluding semi-honest attacker $\mathcal{A}$ in the network. If the cost function is quadratic convex, $\mathcal{A}$ can trivially find the value of a_j just from one iteration. The attacker $\mathcal{A}$ gets the value of $\pi_j(t)$ and $\mu_j(t)$ at $t = 0$:

$$\begin{aligned} \pi_j(0) &= C_j(x_j(0) + s) - C_j(x_j(0)) \\ &= 2a_j x_j(0)s + a_j s^2 + b_j s \end{aligned} \tag{5}$$

$$\begin{aligned} \mu_j(0) &= C_j(x_j(0)) - C_j(x_j(0) - s) \\ &= 2a_j x_j(0)s - a_j s^2 + b_j s \end{aligned} \tag{6}$$

Now, subtracting the equations (5) and (6):

$$2a_j s^2 = \pi_j(0) - \mu_j(0))$$

$$\implies a_j = \frac{\pi_j(0) - \mu_j(0)}{2s^2}$$

Hence, a_j can be found as s is public and known to the attacker. Similarly, the value of b_j can be revealed with few rounds of iteration. Furthermore, if the cost function is non-convex, we can solve a system of non-linear equations received during several rounds to find the cost function parameters (e.g. with a numerical solver).

3. Discussion and Future Work

The security model of a private protocol for EDP follows the ideal-real world paradigm [3]. Informally, an EDP protocol is secure if an adversary can not learn more about individual private inputs in the real world setting than in the ideal world. We assume that all information shared is fixed point values instead of real numbers, so we can convert easily into integers. As any function can be computed securely under a semi-honest model (information theoretic setting) [1], we would like to use a circuit-based approach in our protocol. Our work in progress includes the design and implementation of an auction-based private EDP protocol using different secure multiparty computation primitives like garbled circuits and secret sharing.

References

[1] G. Asharov and Y. Lindell, "A full proof of the bgw protocol for perfectly secure multiparty computation," *Journal of Cryptology*, vol. 30, no. 1, pp. 58–151, 2017.

[2] G. Binetti, A. Davoudi, D. Naso, B. Turchiano, and F. L. Lewis, "A distributed auction-based algorithm for the nonconvex economic dispatch problem," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1124–1132, May 2014.

[3] R. Cramer, I. B. Damgrd, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*, 1st ed. New York, NY, USA: Cambridge University Press, 2015.

[4] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, 2010.

[5] A. Mandal, "Privacy preserving consensus-based economic dispatch in smart grid systems," in *International Conference on Future Network Systems and Security*, vol. CCIS 670. Springer, 2016, pp. 98–110.

[6] S. Yang, S. Tan, and J.-X. Xu, "Consensus based approach for economic dispatch problem in a smart grid," *Power Systems, IEEE Transactions on*, vol. 28, no. 4, pp. 4416–4426, 2013.